

Аннотация к рабочей программе дисциплины «Методы защиты информации»

Рабочая программа дисциплины «Методы защиты информации» разработана для студентов 4 курса, обучающихся по направлению 09.03.04 «Программная инженерия». Дисциплина является обязательной дисциплиной вариативной части учебного плана Б1.В.01.02.

Трудоемкость дисциплины 5 зачетных единиц (180 часов). Дисциплина реализуется в 7 и 8 семестрах. В 7 семестре дисциплина содержит 36 часов лекций, 18 часов лабораторных работ. На самостоятельную работу отводится 54 часа. В 8 семестре дисциплина содержит 24 часа лекций, 12 часов лабораторных работ. На самостоятельную работу отводится 36 часов, из них 27 часов на подготовку к экзамену.

Дисциплина «Методы защиты информации» базируется на дисциплинах «Введение в программную инженерию», «Алгебра и теория чисел», «Технология разработки баз данных». Знания, полученные при ее изучении, будут использованы при подготовке выпускной квалификационной работы.

Цель дисциплины – изучение методов защиты информации в программных системах.

Задачи изучения дисциплины: дать основы

- обеспечения информационной безопасности государства;
- методологии создания систем защиты информации;
- защищенности процессов сбора, передачи и накопления информации;
- методов и средств защищенности и обеспечения информационной безопасности компьютерных систем.

В результате теоретического изучения дисциплины студент должен:

иметь представление:

- о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства, организации, гражданина;
- о методологии создания систем защиты информации;
- о перспективных направлениях развития средств и методов защиты информации;

знать:

- роль и место информационной безопасности в системе национальной безопасности страны;
- угрозы информационной безопасности государства, организации, гражданина;
- современные подходы к построению систем защиты информации;

- компьютерную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;

уметь:

- выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;
- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам.

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
ПК4 владение концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества	Знает	Методы обеспечения информационной безопасности
	Умеет	Использовать методы обеспечения информационной безопасности при работе с информационными технологиями
	Владеет	Методами обеспечения информационной безопасности при поиске информации
ПК5 владение стандартами и моделями жизненного цикла	Знает	Модели жизненного цикла программных систем
	Умеет	Проектировать, разрабатывать и сопровождать программы защиты информации в проектах
	Владеет	Технологиями проверки работоспособности программ защиты информации
ПК16 готовность обосновать принимаемые проектные решения, осуществлять постановку и выполнение экспериментов по проверке их корректности и эффективности	Знает	Математические методы защиты информации от компьютерных вирусов
	Умеет	Использовать антивирусные программы
	Владеет	Методами обновления антивирусных баз
ПК20 способность готовить коммерческие предложения с вариантами решения	Знает	Методы сравнения средств защиты информации
	Умеет	Выбирать подходящие средства для проекта
	Владеет	Методами обоснования выбора

Для формирования вышеуказанных компетенций в рамках дисциплины «Методы защиты информации» применяются следующие методы активного/интерактивного обучения: метод круглого стола.